

PCT/FR 99/02521
9/807614

REC'D 08 NOV 1999

WIPO PCT

FR 99/2521

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 29 OCT. 1999

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE**SIEGE**26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

This Page Blank (uspto)

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

16 OCT. 1998

N° D'ENREGISTREMENT NATIONAL

75 98 12988 -

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT

16 OCT. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

n° du pouvoir permanent 014236

références du correspondant

01 49 69 91 91

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention

☐ demande divisionnaire

☐ certificat d'utilité

☐ transformation d'une demande de brevet européen

☒ demande initiale

☐ brevet d'invention

☐ certificat d'utilité n°

date

Établissement du rapport de recherche

☐ différé

☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui

☒ non

Titre de l'invention (200 caractères maximum)

Composant électronique et procédé pour masquer l'exécution d'instructions ou la manipulation de données

3 DEMANDEUR (S) n° SIREN

code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

S.C.A.
(Société en Commandite par actions)

Nationalité (s) Française

Adresse (s) complète (s)

Pays

Avenue du Pâc de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui

☒ non

Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois

☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS

antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

7812958

n° 014236

TITRE DE L'INVENTION:

Composant électronique et procédé pour masquer l'exécution d'instructions
ou la manipulation de données

LE(S) SOUSSIGNÉ(S)

Lydie BORIN
Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :


- ANGUITA Philippe
- NACCACHE David

domiciliés : Cabinet BALLOT-SCHMIT
16, avenue du Pont Royal
94230 Cachan

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur(s) ou du mandataire

Fait à Cachan, le 16 octobre 1998


BORIN Lydie
Mandataire n° 94-0506
Cabinet BALLOT-SCHMIT

COMPOSANT ÉLECTRONIQUE ET PROCÉDÉ POUR MASQUER
L'EXÉCUTION D'INSTRUCTIONS OU LA MANIPULATION DE
DONNÉES

La présente invention concerne un composant électronique et un procédé pour masquer l'exécution d'instructions ou la manipulation de données.

5 La présente invention concerne plus particulièrement les composants électroniques utilisés dans des applications où l'accès à des services ou à des données est sévèrement contrôlé. De tels composants ont une architecture formée autour d'un microprocesseur et de mémoires. Ils mettent en oeuvre des algorithmes
10 utilisant des données secrètes contenues dans le composant, inaccessibles de l'extérieur. Une donnée secrète peut ainsi servir à valider une transaction électronique telle qu'un achat, sans que cette donnée soit à aucun moment accessible de l'extérieur du
15 composant.

Cependant, l'observation de certains paramètres extérieurs tels que les données échangées avec un système extérieur, ou le courant consommé sur la borne d'alimentation du composant, permet dans certains cas
20 de retrouver des informations concernant le composant, au moyen de traitements statistiques. En particulier, à partir de l'observation en fonction du temps des informations circulant sur le bus de données, en général un bus série, il est possible de faire une
25 corrélation entre ces informations et le déroulement de l'algorithme mis en oeuvre dans le composant.

Il peut être également possible de faire une corrélation de ces informations avec l'observation de la consommation de courant en fonction du temps. Il est
30 alors possible de déduire la valeur d'un bit manipulé

dans une instruction. On sait en effet qu'à un instant donné, la consommation en courant d'une instruction particulière varie selon la valeur "0" ou "1" du bit manipulé.

5 La présente invention a pour but de masquer l'exécution d'instructions ou la manipulation de données dans le composant, afin de rendre stérile l'observation de paramètres externes du composant électronique.

10 Selon l'invention, on prévoit d'interrompre de manière aléatoire l'exécution du programme principal mis en oeuvre par le composant électronique, pour exécuter un programme secondaire. De cette manière, le déroulement du programme change tout le temps. Vu de
15 l'extérieur, il n'est plus possible de faire des traitements statistiques, car les courbes relevées sont toutes décalées temporellement, de manière aléatoire. Si on prend l'exemple de l'observation des données échangées, les temps de réponse de la carte à n'importe
20 quelle commande extérieure changent tout le temps, en sorte qu'il n'est plus possible d'en déduire une quelconque information pertinente.

En ce qui concerne l'observation de la consommation en courant, cette consommation en courant en fonction
25 du temps est elle même découpée, diffusée par rapport à la courbe de consommation normale, en sorte que l'on ne peut obtenir aucune information pertinente.

Ainsi, telle que caractérisée, l'invention concerne un composant électronique comprenant au moins un
30 microprocesseur et des moyens de mémorisation pour exécuter un programme principal.

Selon l'invention, le composant comprend en outre un compteur d'une valeur aléatoire générant en sortie une information pour suspendre l'exécution dudit
35 programme le temps de l'exécution d'un programme secondaire.

Dans un mode de réalisation de l'invention, ce temps d'exécution du programme secondaire est constant. Dans un autre mode de réalisation de l'invention, ce temps d'exécution est variable. Il peut même être aléatoire.

Dans un perfectionnement, on prévoit que ce programme secondaire active des moyens de consommation en courant, qui vont venir fausser la courbe de consommation en courant du composant, rendant le masquage des opérations exécutées et des données manipulées encore plus efficace.

L'invention concerne aussi un procédé de masquage de l'exécution d'instruction ou de la manipulation de données dans un composant électronique.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- la figure 1 représente un schéma-bloc d'un composant électronique selon l'invention; et

- la figure 2 représente une variante du schéma-bloc d'un composant électronique selon une variante de l'invention.

La figure 1 représente un schéma-bloc simplifié d'un composant électronique CI selon l'invention. Il comprend un microprocesseur 1 et des ressources internes qui sont connectés à un bus de données 6. Les ressources internes comprennent notamment des mémoires, dans l'exemple, une mémoire programme 2 et une mémoire de travail 3, un compteur 4 et un générateur 5 d'une valeur aléatoire R.

Le composant électronique CI comprend différentes bornes de connexion externe. Dans l'exemple, c'est un composant à entrée/sortie série de données, avec donc une borne I/O d'entrée/sortie de données. Il comprend aussi une borne de masse VSS, une borne d'alimentation

VCC et des bornes relatives à des signaux de contrôle (non représentés).

Le microprocesseur reçoit des instructions et des données sur un port d'entrée/sortie série 8, connecté à la borne d'entrée/sortie de données en relation avec un système externe.

Le microprocesseur génère en interne différents signaux de contrôle pour gérer les différentes ressources internes.

Parmi ces signaux de contrôle, on a représenté un signal de validation EN du compteur 4, un signal LOAD d'initialisation du compteur et un signal d'activation SEL du générateur aléatoire 5.

Quand il est validé (EN activé), le compteur génère un signal de fin de comptage IT0. Ce signal d'information de fin de comptage est utilisé comme signal d'interruption du microprocesseur. Il est ainsi connecté sur une entrée du port d'interruption 7 du microprocesseur. On notera que l'expression fin de comptage est une expression générale qui veut dire aussi bien que le compteur a fini de compter jusqu'à une valeur déterminée ou que le compteur a fini de décompter à zéro depuis une valeur déterminée.

On notera que dans l'exemple plus particulièrement représenté le compteur est une ressource matérielle.

Le microprocesseur 1 exécute un programme principal contenu en mémoire programme, relativement à des données ou des instructions reçues du port d'entrée/sortie série 8, en relation avec un système externe.

Selon l'invention, l'exécution du programme principal est suspendue à des moments aléatoires, le temps de l'exécution d'un programme secondaire, contenu en mémoire programme.

Pour cela, au début du programme principal, on prévoit une routine d'initialisation du compteur avec une nouvelle valeur aléatoire. En pratique, cette

routine comprend des instructions pour invalider le compteur (EN désactivé), tirer une valeur aléatoire R dans le générateur aléatoire 5, charger (LOAD) cette valeur dans le compteur, puis activer le compteur (EN activé).

Lorsque le compteur a décompté jusqu'à zéro, il active le signal d'information de fin de comptage IT0, ce qui provoque une interruption sur le microprocesseur. L'exécution du programme principal est suspendu le temps de l'exécution (par le microprocesseur) du programme secondaire, correspondant à la routine de gestion de l'interruption considérée.

Le programme secondaire comprend au minimum la séquence déjà vue d'initialisation du compteur, à une nouvelle valeur aléatoire, pour qu'une nouvelle interruption puisse avoir lieu.

Ce programme secondaire peut correspondre à un nombre fixe d'instructions, auquel cas il s'exécute en temps constant. Par exemple, si le programme secondaire comprend seulement les instructions correspondant au tirage d'une nouvelle valeur aléatoire R dans le générateur 5 et au chargement du compteur 4 à cette nouvelle valeur R (initialisation), on a un programme secondaire exécutable en temps constant.

Dans ce cas, en plus de l'exécution du programme principal, on a des bouts de code (correspondant au programme secondaire) exécutés en temps constant à des moments aléatoires.

Dans une variante de l'invention, on prévoit que la durée d'exécution du programme secondaire soit variable.

Dans un premier exemple pratique de réalisation, le programme secondaire prévoit un test sur une donnée binaire, modifiée à chaque passage dans le programme, le nombre d'instructions exécutées ensuite étant fonction du résultat du test. On peut aussi prévoir que

la durée variable d'exécution dépende d'une fonction mathématique. Par exemple, si cette fonction mathématique nécessite un certain nombre de tours de calcul pour arriver au résultat, ce nombre de tours étant fonction des données d'entrée, on aura une durée d'exécution variable, dépendant d'une fonction mathématique. Toutes ces techniques pour arriver à une durée variable sont bien connues.

Dans un autre exemple pratique, on prévoit que cette durée d'exécution variable soit aléatoire. On prévoit dans cet exemple que le programme secondaire comprend la désactivation du compteur, le tirage d'une nouvelle valeur aléatoire, le décomptage jusqu'à zéro de cette valeur dans une boucle de décomptage, puis l'initialisation du compteur à une nouvelle valeur aléatoire.

Dans cette variante, on introduit dans l'exécution du programme principal, des bouts de code exécutés en temps aléatoire à des moments aléatoires.

En pratique, de nombreuses variantes de l'invention sont possibles.

Notamment, pour ne pas trop dégrader le temps d'exécution du programme principal, on peut prévoir de limiter dans le temps la durée totale des retards dus à l'exécution du ou des programmes secondaires.

Dans un autre mode de réalisation de l'invention, on prévoit non seulement de suspendre l'exécution du programme principal à des moments aléatoires, mais aussi de prévoir une consommation en courant supplémentaire, qui va brouiller la consommation en courant due à l'exécution du programme principal.

Cette consommation en courant supplémentaire peut être due, de façon instantanée, à des instructions prévues dans le programme secondaire. Par exemple, on peut prévoir dans ce programme secondaire, d'exécuter

des tours de calcul d'un algorithme, par exemple d'un algorithme de cryptographie.

5 A cette exécution va correspondre une consommation en courant instantanée, c'est à dire le temps de l'exécution de l'instruction, qui va brouiller la consommation normale du programme principal en venant s'intercaler dans la consommation de courant normale en fonction du temps due à l'exécution du programme principal.

10 On peut aussi prévoir que cette consommation de courant supplémentaire ait un effet durable pendant un certain temps. Le programme secondaire prévoit alors d'activer des moyens de consommation de courant, qui vont consommer du courant au moins un certain temps, pendant l'exécution des instructions suivantes du programme secondaire et du programme principal.

Un schéma-bloc d'un composant électronique correspondant à ce deuxième mode de réalisation de l'invention est représenté sur la figure 2.

20 En plus des éléments déjà décrits qui portent les mêmes références que sur la figure 1, le composant électronique comprend une pompe de charges 9.

25 Cette pompe de charges est normalement prévue pour fournir une haute tension VPP de programmation et/ou d'effacement à partir de la tension d'alimentation VCC pour permettre la programmation et/ou l'effacement de données dans une mémoire non volatile programmable et/ou effaçable électriquement, comme par exemple les mémoires communément appelées mémoires EPROM, EEPROM ou encore flash EPROM. Dans l'invention, cette pompe de charges est associée à la mémoire programme.

30 Dans l'exemple, elle est activée par un signal d'écriture WE de la mémoire programme.

35 Une telle pompe a comme caractéristique connue de consommer beaucoup de courant pendant le temps d'établissement de la haute tension en sortie et le

temps de la programmation ou de l'effacement, ce qui peut être de l'ordre de quelques millisecondes. En activant une telle pompe, par exemple, en prévoyant une instruction de programmation dans le programme
 5 secondaire, on surimpose donc une forte consommation en courant qui va masquer la consommation des instructions suivantes du programme secondaire et du programme principal.

10 L'invention ne se limite pas aux modes de réalisation ou aux variantes décrits. Elle couvre toute utilisation de moyens pour suspendre le programme principal à des moments aléatoires pendant un temps qui peut-être fixe, variable ou aléatoire, avec ou sans l'utilisation de moyens pour ajouter une consommation
 15 en courant supplémentaire.

Avec un tel masquage ou brouillage en utilisant l'une quelconque des variantes de l'invention ou une combinaison de celles-ci, aucun traitement statistique ne devient possible.

20 En pratique, le choix de tel ou tel programme secondaire peut dépendre de l'application à laquelle le composant électronique est destiné.

L'invention s'applique à tous les composants comprenant au moins un compteur et un générateur
 25 aléatoire. Pour un composant électronique donné, le choix de tel ou tel programme secondaire dépend des ressources du composant considéré, de l'efficacité en rapport avec l'application considérée.

On peut aussi prévoir d'utiliser différents programmes secondaires, ce qui permet de mélanger les genres, pour améliorer le brouillage, le choix du programme secondaire à exécuter se faisant alors en
 30 début de routine d'interruption.

Un tel composant est tout particulièrement utilisable dans les cartes à puces, pour améliorer leur
 35 inviolabilité.

REVENDEICATIONS

1. Composant électronique comprenant au moins un microprocesseur (1) et des moyens de mémorisation (2, 3) pour exécuter un programme principal, caractérisé en ce qu'il comprend en outre un compteur (4) d'une valeur aléatoire (R), ledit compteur générant en sortie un signal d'information de fin de comptage (IT0) pour suspendre l'exécution dudit programme principal- le temps de l'exécution d'un programme secondaire par le microprocesseur.

2. Composant électronique selon la revendication 1, caractérisé en ce que le temps d'exécution du programme secondaire est constant.

3. Composant électronique selon la revendication 1, caractérisé en ce que le temps d'exécution du programme secondaire est variable.

4. Composant électronique selon la revendication 3, caractérisé en ce que le temps d'exécution du programme secondaire est aléatoire.

5. Composant électronique selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre des moyens consommateur de courant activés par le programme secondaire.

6. Composant électronique selon la revendication 5, caractérisé en ce que ces moyens consommateur de courant comprennent une pompe de charges (9).

7. Composant électronique selon la revendication 5 ou 6, caractérisé en ce que ces moyens comprennent des instructions entraînant une consommation instantanée.

8. Procédé pour masquer l'exécution d'opérations ou la manipulation de données dans un composant électronique (CI) comprenant un microprocesseur (1) et des moyens de mémorisation (2, 3) pour exécuter un programme principal, caractérisé en ce que ce procédé consiste à utiliser un générateur (5) d'une valeur aléatoire (R) et un compteur (4) pour suspendre l'exécution du programme principal à des instants aléatoires, le temps de l'exécution d'un programme secondaire.

9. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur (4) avec cette nouvelle valeur et à autoriser le décomptage avant de retourner à l'exécution du programme principal.

10. Procédé selon la revendication 8, caractérisé en ce que le programme secondaire est exécutable en temps aléatoire.

11. Procédé selon la revendication 10, caractérisé en ce que le programme secondaire consiste à invalider le compteur (4), à tirer une nouvelle valeur aléatoire (R), à décompter jusqu'à zéro cette nouvelle valeur aléatoire dans une boucle du programme secondaire, puis à tirer une nouvelle valeur aléatoire (R), à initialiser le compteur à cette nouvelle valeur et à

activer le compteur avant de retourner à l'exécution du programme principal.

12. Procédé selon l'une quelconque des revendications 8 à 11, caractérisé en ce que le programme secondaire active en outre des moyens de consommation de courant.

13. Procédé selon la revendication 12, caractérisé en ce que les dits moyens de consommation de courant comprennent une pompe de charges (9).

14. Procédé selon la revendication 12 ou 13, caractérisé en ce que ces moyens comprennent des instructions provoquant une consommation en courant instantanée.

15. Procédé selon l'une quelconque des revendications 8 à 14, caractérisé en ce qu'il comprend différents programmes secondaires.

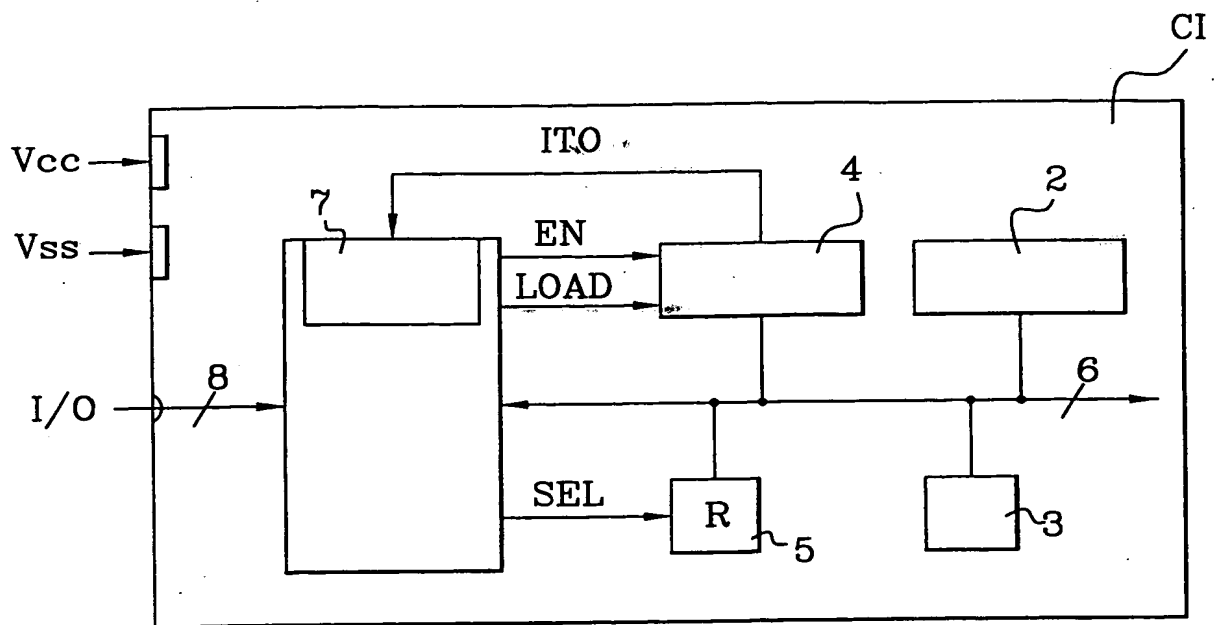


FIG.1

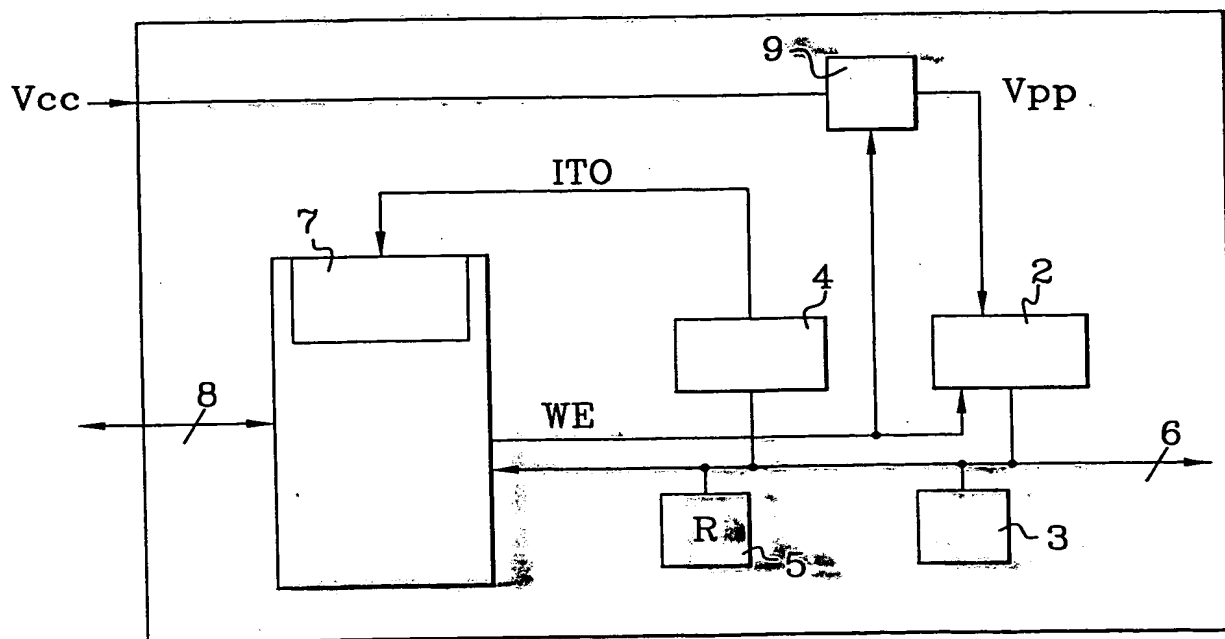


FIG.2